IN THE CLAIMS

Please amend the claims as follows:

1. (Original) A method of providing Internet Protocol Security (IPSec) to a plurality of target hosts in a cluster of data processing systems which communicate with a network through a routing communication protocol stack utilizing a dynamically routable Virtual Internet Protocol Address (DVIPA), the method comprising:

negotiating security associations (SAs) associated with the DVIPA utilizing an Internet Key Exchange (IKE) component associated with the routing communication protocol stack; and

distributing information about the negotiated SAs to the target hosts to allow the target hosts to perform IPSec processing of communications from the network utilizing the negotiated SAs.

2. (currently amended) The ~~A~~ method according to Claim 1, wherein the routing communication protocol stack further carries out the steps of:

receiving a communication from the network;

determining if the communication is an IPSec communication to the DVIPA; and

routing the received communication to one of the target hosts.

3. (currently amended) The ~~A~~ method according to Claim 2, wherein the step of determining if the communication is an IPSec communication comprises the steps of:

evaluating a destination address in the IP header of a received datagram of the communication; and

determining if the destination address is a dynamic VIPA.

4. (currently amended) The ~~A~~ method according to Claim 3, wherein the step of evaluation a destination address is preceded by the steps of:

determining if the destination address is encrypted; and

decrypting the received communication utilizing an SA associated with the IPSec communication to decrypt a Transmission Control Protocol (TCP) header of the datagram.

5. (currently amended) The ~~A~~ method according to Claim 4, further comprising the step of determining a location of the TCP header in the received communication based on whether the IPSec SA is in transport mode or tunnel mode.

6. (currently amended) The ~~A~~ method according to Claim 3, wherein the routing communication protocol stack further carries out the step of bypassing inbound filtering if the communication is an IPSec communication to the DVIPA.

7. (currently amended) The ~~A~~ method according to Claim 3, wherein the routing communication protocol stack further carries out the steps of:

inbound filtering the communication if the communication is an IPSec communication; and

encapsulating the filtered inbound communication in a generic routing format; and

wherein the step of routing comprises routing the encapsulated communication to the one of the target hosts; and

wherein a communication protocol stack of the one of the target hosts carries out the steps of:

bypassing inbound filtering of the routed encapsulated communication; and decapsulating the routed encapsulated communication.

8. (currently amended) The ~~A~~ method according to Claim 7, wherein the step of inbound filtering further comprises the steps of:

performing a tunnel check on the received communication; and

rejecting the received communication so as to not route the received communication to the one of the target hosts based on the results of the tunnel check.

9. (currently amended) The ~~A~~ method according to Claim 2, wherein the routing communication protocol stack further carries out the steps of:

performing a replay sequence number check on the received communication; and

rejecting the communication so as to not route the received communication to the one of the target hosts based on the results of the replay sequence number check.

10. (currently amended) The ~~A~~ method according to Claim 2, wherein the step of routing comprises the steps of:

selecting a target host from the plurality of target hosts based on entries in a distributed connection table associated with the DVIPA; and

sending the received communication to the selected target host over a trusted link.

11. (currently amended) The ~~A~~ method according to Claim 1, wherein the information about the negotiated SAs comprises the SAs and wherein the step of distributing further comprises the step of storing the distributed SAs in a shadow cache of communication protocol stacks of the target hosts.

12. (currently amended) The ~~A~~ method according to Claim 11, wherein the target hosts further carry out the step of IPSec processing communications to the DVIPA utilizing the SAs in the shadow cache.

13. (currently amended) The ~~A~~ method according to Claim 12, further comprising the step of providing an inbound lifesize count from the communication protocol stacks of the target hosts to the routing communication protocol stack.

14. (currently amended) The ~~A~~ method according to Claim 13, wherein the IKE refreshes the SAs associated with the DVIPA based on the inbound lifesize count provided by the communication protocol stacks of the target hosts.

15. (currently amended) The ~~A~~ method according to Claim 13, wherein the step of providing an inbound lifesize count comprises the step of sending a cross coupling facility (XCF) message identifying the inbound lifesize count to the routing communication protocol stack.

16. (currently amended) The ~~A~~ method according to Claim 15, wherein the step of sending an XCF message identifying the inbound lifesize count comprises the step of periodically sending a XCF message identifying the inbound lifesize count for a plurality of IPSec processed communications.

17. (currently amended) The ~~A~~ method according to Claim 16, wherein the plurality of IPSec processed communications comprises a percentage of a total lifesize count associated with an SA.

18. (currently amended) The ~~A~~ method according to Claim 17, further comprising the step of dynamically establishing the percentage of the total lifesize count based on whether the IKE has previously refreshed the SA prior to expiration of a lifesize count threshold associated with the SA.